

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

EDWARD WOOTEN and SARKIS
OGANYAN, individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

BIOLIFE PLASMA SERVICES L.P. and
TAKEDA PHARMACEUTICALS U.S.A.,
INC.,

Defendants.

No. 1:25-cv-00099-KES-SKO

ORDER GRANTING DEFENDANTS'
MOTION TO DISMISS

Doc. 19

Plaintiffs Evan Wooten and Sarkis Oganyan proceed on their first amended class action complaint (“FAC”), on behalf of themselves and others, against defendants BioLife Plasma Services L.P. (“BioLife”) and Takeda Pharmaceuticals U.S.A., Inc. (“Takeda”). Doc. 17 (“FAC”). Plaintiffs allege that, when they created accounts on BioLife’s website, third-party trackers installed by defendants, and operated by third-parties Snap and Salesforce, captured their email addresses and IP addresses without their consent, in violation of the California Invasion of Privacy Act (“CIPA”). Defendants move to dismiss the FAC pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), and 12(b)(6). Doc. 19.¹ For the reasons set forth below,

¹ Defendants’ motion did not initially seek to dismiss plaintiffs’ claims under Rule 12(b)(1) for lack of subject matter jurisdiction. *See* Doc. 19. However, following the filing of defendants’ motion, the Court granted the parties’ request to submit supplemental briefing regarding whether plaintiffs have standing under Article III to bring their claims. Docs. 24, 25.

defendants' motion is granted, and this action is dismissed without prejudice.

I. Background²

Plaintiffs' FAC alleges the following. BioLife and Takeda operate more than 200 blood plasma donation centers across the United States, serving thousands of monthly donors. FAC ¶ 32. In exchange for donations, donors receive monetary compensation. *Id.* A prospective donor cannot donate until they make an account by visiting BioLife's website. *Id.* ¶ 33. When signing up for an account through the website, prospective donors are presented with an online form requesting that they provide their first name, last name, email address, and zip code. *Id.* ¶ 41. Once a user enters the information in the online form and clicks "next," but before the user completes the account creation process, third party trackers installed by defendants intercept the user's email address, the user's IP address, and the fact that the user visited the website.³ *Id.* ¶ 42. The email address is captured in an encrypted format but is readily decodable and traceable to the individual user. *Id.* ¶¶ 47–55. The IP address allows the third parties to determine the device's state, city, zip code, and approximate latitude and longitude. *Id.* ¶ 62.

The intercepted email address and IP address together enable the third parties to link users' identities across multiple websites and apps, through a process known as "ID bridging." *Id.* ¶ 72. Through ID bridging, the third parties have the ability to "follow [users] all over the internet and feed them advertisements." *Id.* ¶ 77. The collected data can also be used for research and marketing purposes for both defendants and the third parties. *Id.* ¶¶ 82, 86–90; 92–100.

Plaintiff Wooten alleges that he created a BioLife account sometime in February 2023; plaintiff Oganyan alleges that he did so on or about January 28, 2024. *Id.* ¶¶ 6, 8. In creating their accounts, plaintiffs input the requested information on the online form, including their email addresses. *Id.* Wooten states he has continued to access his account through the website as recently as November 2024, and Oganyan states he did so as recently as February 2025. *Id.*

² The recitation of facts is based on the allegations contained in the FAC, Doc. 17, the truth of which the Court accepts for purposes of resolving the motion to dismiss. *See Boquist v. Courtney*, 32 F.4th 764, 772 (9th Cir. 2022).

³ The trackers are (i) Evergage, which is owned and operated by Salesforce, and (ii) the Snap Pixel, which is owned and operated by Snap. FAC ¶ 38.

1 Plaintiffs contend that they did not consent to the collection of their email and IP addresses prior
 2 to completing the account creation process, and that they were not aware the collection was
 3 occurring. *Id.* Plaintiffs allege defendants used the intercepted email and IP addresses for
 4 marketing, advertising, and data analytics purposes. *Id.* ¶ 125. Plaintiffs do not allege that they
 5 received targeted advertising, linked to the collection, since creating their accounts.

6 On January 22, 2025, plaintiff Wooten filed a complaint asserting violations of:
 7 (1) CIPA’s wire-tapping provision under California Penal Code § 631(a), and (2) CIPA’s pen-
 8 register provision under California Penal Code § 638.51(a). Doc. 1. Defendants filed an initial
 9 motion to dismiss on April 4, 2025. Doc. 13. In response, Wooten filed the operative FAC,
 10 adding plaintiff Oganyan and alleging the same causes of action with additional factual
 11 allegations. Doc. 17. Defendants then filed a motion to dismiss on June 6, 2025. Doc. 19.
 12 Following the Ninth Circuit’s decision in *Popa v. Microsoft Corp.*, --- F.4th ---, 2025
 13 WL 2448824 (9th Cir. Aug. 25, 2025), the Court granted the parties’ request to submit
 14 supplemental briefing regarding whether plaintiffs have Article III standing to bring their claims.
 15 Docs. 24, 25. The Court held oral argument on October 14, 2025. Doc. 33. For the reasons
 16 explained below, defendants’ motion is granted as plaintiffs fail to establish standing under
 17 Article III, and this action is dismissed without prejudice.

18 **II. Legal Standard**

19 The Court evaluates challenges to Article III standing under Rule 12(b)(1), which governs
 20 motions to dismiss for lack of subject matter jurisdiction. *See Maya v. Centex Corp.*, 658 F.3d
 21 1060, 1067 (9th Cir. 2011). A motion to dismiss under Rule 12(b)(1) may be facial or factual.
 22 *San Diego Cnty. Credit Union v. Citizens Equity First Credit Union*, 65 F.4th 1012, 1028 (9th
 23 Cir. 2023). “In a facial attack, the challenger asserts that the allegations contained in a complaint
 24 are insufficient on their face to invoke federal jurisdiction.” *Safe Air for Everyone v. Meyer*,
 25 373 F.3d 1035, 1039 (9th Cir. 2004) (citing *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000)).
 26 “The district court resolves a facial attack as it would a motion to dismiss under Rule 12(b)(6):
 27 [a]ccepting the plaintiff’s allegations as true and drawing all reasonable inferences in the
 28 plaintiff’s favor, the court determines whether the allegations are sufficient as a legal matter to

1 invoke the court's jurisdiction.” *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). “By
 2 contrast, in a factual attack, the challenger disputes the truth of the allegations that, by
 3 themselves, would otherwise invoke federal jurisdiction.” *Safe Air for Everyone*, 373 F.3d at
 4 1039. In a factual challenge, the court does not simply accept the allegations in the complaint as
 5 true. *Leite*, 749 F.3d at 1121. Once the truth of the allegations is challenged, the responding
 6 party needs to support the jurisdictional allegations with “competent proof.” *Id.* Here, defendants
 7 make a facial attack as they argue that the allegations contained in the complaint are insufficient
 8 on their face to establish standing. *See* Doc. 27.

9 **III. Discussion**

10 To establish standing, plaintiffs must show “(i) that [they] suffered an injury in fact that is
 11 concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the
 12 defendant; and (iii) that the injury would likely be redressed by judicial relief.” *TransUnion LLC*
 13 *v. Ramirez*, 594 U.S. 413, 423 (2021) (citing *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 560–61
 14 (1992)). A concrete injury “must actually exist;” it must be “real,” and not “abstract.” *Spokeo,*
 15 *Inc. v. Robins*, 578 U.S. 330, 340 (2016). But “Congress’ role in identifying and elevating
 16 intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact
 17 requirement whenever a statute grants a person a statutory right and purports to authorize that
 18 person to sue to vindicate that right.” *Id.* at 341. In other words, plaintiffs’ allegations that
 19 defendants violated the California Invasion of Privacy Act do not automatically create a concrete
 20 injury in the Article III context. Rather, a concrete injury may be intangible if it “has a close
 21 relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in
 22 English or American courts.” *Id.* In determining whether alleged privacy intrusions bear such a
 23 relationship, courts mainly consider “the nature of the information at issue.” *In re Yahoo Mail*
 24 *Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014). “[I]n data breach cases, courts must examine
 25 the nature of the specific information at issue to determine whether privacy interests were
 26 implicated at all.” *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1050 (N.D. Cal. 2022).

27 Plaintiffs have failed to establish that defendants’ one-time collection and dissemination
 28 of plaintiffs’ IP and email addresses, through the third-party trackers, sufficiently impacts

1 plaintiffs' privacy interests to give rise to a concrete injury. Courts have held that there is no
 2 legally protected privacy interest in an IP address or, in many contexts, in such relatively
 3 quotidian private information as an email address. *See Khamooshi v. Politico LLC*, 786 F. Supp.
 4 3d 1174 (N.D. Cal. 2025); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034 (N.D. Cal. 2022); *Mikulsky v.*
 5 *Noom, Inc.*, 682 F. Supp. 3d 855 (S.D. Cal. 2023); *Liau v. Weee! Inc.*, 23-civ-1177 (PAE), 2024
 6 WL 729259 (S.D.N.Y. Feb. 22, 2024). Concrete intangible harms must also bear a close
 7 relationship to traditionally recognized harms. *See Spokeo*, 578 U.S. at 341.

8 As the Ninth Circuit recently clarified, "there existed no free-roaming privacy right at
 9 common law but rather four discrete torts that protected specific kinds of privacy-related harms . .
 10 . 'intrusion upon seclusion, appropriation of another person's name or likeness, publicity given to
 11 another person's private life, and publicity that places one in a false light.'" *Popa v. Microsoft*
 12 *Corp.*, --- F.4th ---, 2025 WL 2448824, at *6 (9th Cir. Aug. 26, 2025) (quoting *Nabozny v. Optio*
 13 *Sols. LLC*, 84 F.4th 731, 735 (7th Cir. 2023)). At oral argument, plaintiffs argued that defendants
 14 committed an intrusion upon seclusion when the third-party trackers allegedly intercepted their IP
 15 and email addresses. The Court disagrees. To show intrusion upon seclusion, a plaintiff must
 16 show "an intentional interference with his interest in solitude or seclusion, either as to his person
 17 or as to his private affairs or concerns, of a kind that would be *highly offensive to a reasonable*
 18 *man.*" *Id.* at *5 (quoting *Nayab v. Cap. One Bank (USA), N.A.*, 942 F.3d 480, 491 (9th Cir. 2019)
 19 (emphasis added)). Disclosure of one's email address and IP address, without more, does not
 20 bear similarity to the "highly offensive" interferences or disclosures that were actionable at
 21 common law. *See id.*; *Khamooshi*, 786 F. Supp. 3d at 1180; *Zynga*, 600 F. Supp. 3d at 1049; *Xu*
 22 *v. Reuters News & Media Inc.*, 24-civ-2466 (PAE), 2025 WL 488501 (S.D.N.Y. Feb. 13, 2025);
 23 *Cooper v. Bonobos, Inc.*, 21-cv-854 (JMF), 2022 WL 170622, at *4 (S.D.N.Y. Jan. 19, 2022).

24 Plaintiffs rely on the Ninth Circuit's decision in *In re Facebook, Inc. Internet Tracking*
 25 *Litigation*, 956 F.3d 589 (9th Cir. 2020). There, it was alleged that, when a user created a
 26 Facebook account, Facebook placed more than ten cookies on the user's browser that tracked the
 27 user's browsing history even after the user logged out of Facebook and visited other websites.
 28 *Facebook*, 956 F.3d at 596. Facebook used such information in combination with the user's

personal Facebook profiles, which could include employment history and political and religious affiliations, to gain a cradle-to-grave profile without the user’s consent. *Id.* at 599. The court held that allegations of data collection performed “in order to receive and compile [the user’s] personally identifiable browsing history . . . no matter how sensitive or personal” constituted a “clear invasion of the historically recognized right to privacy” sufficient to establish Article III standing. *Id.* at 598–99.

In arguing that the one-time collection, and dissemination to Snap and Salesforce, of a user’s IP address and email address establishes a concrete injury, plaintiffs misinterpret *Facebook*. *Facebook* held that a dissemination of personal information *may* result in a concrete injury, as the right to privacy “encompass[es] the individual’s control of information concerning his or her person,” *Facebook*, 956 F.3d at 598 (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)), but the invasive nature of the information collected was crucial to *Facebook*’s holding. The *Facebook* decision “accounted for the individual circumstances giving rise to the plaintiffs’ alleged injuries rather than simply greenlighting a per se rule for privacy statutes.” *Popa*, 2025 WL 2448824, at *8. Here, plaintiffs allege a one-time collection of their IP and email addresses, but they do not allege that the third-party trackers collected any other “embarrassing, invasive, or otherwise private information.”⁴ *Id.* at *5.

⁴ The other cases plaintiffs cite are also distinguishable from this case. *See* Doc. 28. While several of them involve the collection of an IP address or an email address, the information collected in those cases always included something more. *See Deivaprakash v. Condé Nast Digital*, --- F. Supp. 3d ---, 2025 WL 2541952, at *1 (N.D. Cal. Sept. 4, 2025) (finding allegations “likely satisfy” Article III standing where users alleged cookies monitored users’ behavior across internet beyond their use of defendant’s website, and compiled comprehensive profiles reflecting users’ geographic locations, incomes, and preferences); *Atkins v. Amplitude, Inc.*, No. 24-cv-04913-RFL, 2025 WL 2521732, at *1 (N.D. Cal. Sept. 2, 2025) (finding standing where app allegedly collected “timestamped geolocation information, device IDs, device fingerprint data . . . search terms input to the app, products placed in [consumer’s] cart” and may reveal “consumer’s religious affiliation, sexual orientation, [or] medical condition”); *Gabrielli v. Haleon US Inc.*, No. 25-cv-02555-WHO, 2025 WL 2494368, at *6 (N.D. Cal. Aug. 29, 2025) (finding standing where cookies allegedly tracked “browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, [and] referring URLs”); *Salazar v. National Basketball Association*, 118 F.4th 533, 537–38 (2d Cir. 2024) (finding standing where Meta Pixel allegedly tracked users’ personal viewing information including the (1) title of the NBA.com video a user watched, (2) that video’s URL, and (3) the user’s Facebook ID, to send user targeted advertising);

1 Plaintiffs also do not sufficiently allege any *actual* injury. Rather, they allege that the
 2 third-party trackers have the *capability* to use these pieces of information to engage in ID
 3 bridging, which could then result in targeted advertising and could contribute to defendants’
 4 marketing, advertising, and data analytics efforts. *See* FAC ¶¶ 77, 81. But plaintiffs do not allege
 5 that defendants themselves took any such actions. Nor do plaintiffs specifically allege that they
 6 were subject to any such targeted advertising. *See Doe I v. Google LLC*, 741 F. Supp. 3d 828,
 7 839 (N.D. Cal. 2024) (“[I]nstead of offering factual allegations about how the plaintiffs’ various
 8 providers are *actually* using Google’s products, the plaintiffs allege hypothetical examples—
 9 based on the generic product descriptions—of how various product features could be used in
 10 ways that could result in privacy violations.”); *Xu*, 2025 WL 488501, at *3 (“[T]he complaint
 11 does not allege that [plaintiff] received any targeted advertising or was otherwise affected, much
 12 less that [plaintiff] was concretely harmed by any such advertising.”). Alleged retention of
 13 noninvasive information alone is insufficient to establish Article III standing. *See Phillips v. U.S.*
 14 *Customs & Border Prot.*, 74 F.4th 986, 993 (9th Cir. 2023) (“Where we have held that the
 15 retention of illegally obtained records resulted in a concrete injury, we have always identified
 16 something beyond retention alone that resulted in an injury of the sort recognized by the Supreme
 17 Court, such as . . . a violation of the common law right to privacy.”).

18 Plaintiffs fail to establish that the one-time collection of their IP and email addresses is a
 19 concrete harm, and they have therefore failed to establish standing under Article III. The FAC
 20 must therefore be dismissed without prejudice. *See Barke v. Banks*, 25 F.4th 714, 721 (9th Cir.
 21 2022) (“[D]ismissals for lack of Article III jurisdiction must be entered without prejudice because
 22 a court that lacks jurisdiction is ‘powerless to reach the merits.’”) (quoting *Fleck & Assocs., Inc.*
 23 *v. Phoenix, City of, an Ariz. Mun. Corp.*, 471 F.3d 1100, 1106–07 (9th Cir. 2006)).

24 ///

25 ///

26 ///

27 _____
 28 *Salazar v. Paramount Global*, 133 F.4th 642, 647 (6th Cir. 2025) (finding standing where Pixel
 allegedly tracked user’s private video-viewing history).

IV. Conclusion and Order:

Accordingly:

1. Defendants' motion to dismiss, Doc. 19, is GRANTED;
2. This action is DISMISSED without prejudice; and
3. The Clerk of Court is directed to CLOSE this case.

IT IS SO ORDERED.

Dated: October 22, 2025


UNITED STATES DISTRICT JUDGE